(U//FOUO) Dragons, Shrimp, and XKEYSCORE: Tales from the Land of Brothers Grimm

FROM: European Cryptologic Center, SIGDEV (F22)

Run Date: 04/13/2012

(S//REL) The European Cryptologic Center (ECC) sits quietly nestled amongst vineyards and farmlands on

E ECC

the outskirts of Darmstadt, Germany. To the passing motorist, the facility looks like many of the other random U.S. government facilities in the area, with one exception. One can almost hear a discernable buzz of activity from the analysts of the ECC executing queries, authoring fingerprints, and

ECC		

consuming metadata garnered from XKEYSCORE (XKS). In the past three months, the ECC has tripled, and even quadrupled in some cases, the number of queries performed, the number of items pushed to PINWALE, and the number of sessions viewed. And these numbers continue to grow.*

(S//REL) What has been the cause of this flurry of success? The ECC points to a recent XKS training blitz in support of the Analytic Modernization Outreach Campaign to encourage discovery. In early March, ECC SIGDEV analysts held an XKS Circuit Training event designed to expose analysts to five, 20-minute one-on-one sessions in a circuit-type environment. This "speed dating" for XKS consisted of five stations covering topics titled "Intro to the GUI and Basic Queries," "Metadata Setup and Manipulation," "Content and Manipulation of Results," "Introduction to Fingerprints," and "Introduction to Microplugins."

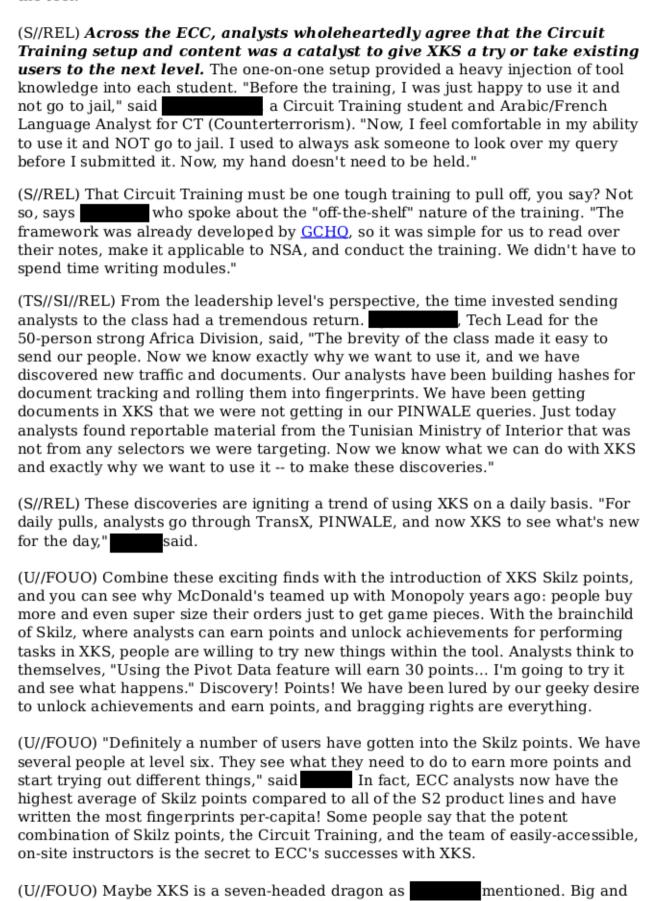
(S//REL) Over four days, 68 students were walked through these topics with five different instructors, able to ask specific questions and get more comfortable with the tool. "Everyone likes a new toy, and there was a lot of excitement about it. They will at least try it against their target and see what they will get out of it," said one of the instructors and a SIGDEV Analyst embedded in Africa Division.

(S//SI//REL) With traditional targeting, analysts cast their nets wide into the murky waters of network traffic and haul in anything that gets caught in the net. We are like Forrest Gump on his shrimping boat off the coast of Alabama pulling in a boot, toilet seat, seaweed, and there they are... three shrimp! We burn up a lot of resources getting those shrimp, those reportable documents or metadata used to expand target knowledge, and we deal with tons of toilet seats, the spam and other junk. Then, we repeat the same process and hopefully catch enough "shrimp" to have ourselves a little cocktail. XKS has become so important because with it, analysts can downsize their gigantic shrimping nets to tiny, handheld goldfish-sized nets and merely dip them into the oceans of data, working smarter and scooping out exactly what they want.

(U//FOUO) And a short, two-hour class is an easy gamble of time for the hopes of being able to work smarter and more efficiently. ECC analysts have been trading in their old nets for new ones and are thrilled with their catches. Discovery can only occur if people are willing to try new things, and more of our analysts are getting comfortable with leaping into the relatively unknown world of XKS.

(U//FOUO) "The first time I saw XKS, I said, 'Whoa!!' It is intimidating because you open it up and you see all these queries and fields," said "We took the students from that response to being able to approach it and navigate around in it. They see it differently now and know it's not a seven-headed dragon." This gentle introduction has definitely enabled analysts to ease into XKS and get more comfortable, and with that it has radically changed the overall mentality towards

the tool.



scary? Sure. Strong and powerful? Oh yeah. But, the ECC is taming it, and it is ours

to do with whatever we like, including catchi

(U//FOUO) POC:

* (S//REL) Here are charts to illustrate the point:

. .